CLAIMS

What is claimed is:

1. A method for facilitating the reauthentication of a user using a client computer to a server computer comprising the steps of:

(a) receiving confidential information from the client computer;

(b) establishing a first communication session between the client computer and the server computer;

(c) generating a key;

(d) encrypting the confidential information with the key to create encrypted confidential information;

(e) storing the encrypted confidential information on the server computer;

(f) transmitting the key to the client computer; and

(g) deleting the key on the server computer.

2. The method of claim 1 further comprising the steps of:

(h) establishing a second communication session after deleting the key on the server computer;

(i) receiving the key associated with the encrypted confidential information from the client computer during the second communication session; and

(j) using the key by the server computer to decrypt the encrypted confidential information.

3. The method of claim 1 wherein step (e) further comprises the step of:

(e-a) creating an identifier by the server computer prior to transmitting the key to the client computer; and

(e-b) storing the identifier on the server computer.

4. The method of claim 2 wherein step (h) further comprises the steps of:

(h-a) receiving an identifier associated with the first communication session from the client computer during the second communication session before using the key to decrypt the encrypted confidential information; and

(h-b) using the identifier to locate the encrypted confidential information before using the key to decrypt the encrypted confidential information.

5. The method of claim 2 further comprising the step of establishing the second communication session between the client computer and the server computer upon termination of the first communication session.

6. The method of claim 2 further comprising the steps of:

(k) creating a second key during the second communication session;

(l) creating a second identifier during the second communication session;

(m) encrypting the confidential information with the second key to create second encrypted confidential information;

(n) storing the encrypted confidential information and the second identifier on the server computer;

(o) transmitting the second key and the second identifier to the client computer; and

(p) deleting the second key on the server computer.

7. The method of claim 1 wherein encrypting of the confidential information and the key further comprises performing an exclusive OR operation on the confidential information and the key.

8. The method of claim 1 further comprising enabling access to the encrypted confidential information for a predetermined amount of time.

9. The method of claim 3 wherein the identifier further comprises a pointer to the encrypted confidential information.

10. The method of claim 1 wherein the encrypted confidential information is stored in a database.

11. The method of claim 1 wherein the confidential information is a password.

12. The method of claim 3 wherein the identifier is a session identifier.

13. A system for facilitating reauthentication of a user using a client computer to a server computer, the system comprising:

(a) a client computer; and

(b) a server computer comprising

a memory,

a key generator,

a key destroyer,

an encryptor, and

a decryptor,

the server computer in electrical communication with the client computer;

wherein the server computer receives confidential information from the client computer during a first communication session between the server computer and the client computer,

wherein the key generator generates a key,

wherein the encryptor encrypts confidential information received from the client computer with the key to create encrypted confidential information,

wherein the encryptor stores the encrypted confidential information in the memory of the server computer,

wherein the server computer transmits the key to the client computer, and

wherein the key destroyer destroys the key following transmission to the client computer.

14. The system of claim 13 wherein the server computer receives the key during a second communication session.

15. The system of claim 13 wherein the decryptor decrypts the encrypted confidential information in the memory using the key.

16. The system of claim 13 wherein the confidential information is personal information associated with a user of the client computer.

17. The system of claim 13 further comprising an identifier generator that generates an identifier.

18. The system of claim 17 wherein the identifier generator associates the identifier with the encrypted confidential information.

19. The system of claim 13 wherein the identifier is a session identifier.

20. A system for facilitating the reauthentication of a client computer to a server computer, the system comprising:

(a) a client computer; and

(b) a server computer comprising

a memory,

a key generator,

a key destroyer,

an identifier generator,

an encryptor, and

a decryptor,

the server computer in electrical communication with the client computer;

wherein the server computer receives confidential information from the client computer during a first communication session between the server computer and the client computer,

wherein the key generator generates a key,

wherein the encryptor encrypts confidential information received from a client with the key to create encrypted confidential information,

wherein the identifier generator generates an identifier,

wherein the server computer stores the encrypted confidential information and the identifier in the memory of the server computer,

wherein the server computer transmits the key and the identifier to the client computer,

wherein the key destroyer destroys the key following transmission to the client computer, and

wherein the server computer receives the key and the identifier during a second communication session to enable the decryptor to decrypt the encrypted confidential information in the memory.

21. A method for facilitating the reauthentication of a client computer to a server computer comprising the steps of:

(a) establishing a first communication session between a client computer and a server computer;

(b) receiving confidential information from the client computer;

(c) creating an identifier by the server computer to identify the first communication session after receiving the confidential information;

(d) encrypting the confidential information with a key to create encrypted confidential information;

(e) storing the encrypted confidential information and the identifier in a table in memory of the server computer;

(f) transmitting, by the server computer, the key and the identifier to the client computer;

(g) deleting, by the server computer, the key from the memory of the server computer;

(h) establishing a second communication session between the client computer and the server computer upon termination of the first communication session;

(i) receiving, from the client computer, during the second communication session, the identifier that identifies the first communication session;

(j) receiving, from the client computer, during the second communication session, the key associated with the encrypted confidential information;

(k) using the identifier to determine the location of the encrypted confidential information in the table; and

(l) decrypting, by the server computer, the encrypted confidential information using the key received from the client computer during the second communication session.

22. A computer system for facilitating reestablishment of communications between a client computer and a server computer comprising:

(a) means for receiving confidential information from a client computer during a first communication session;

(b) means for encrypting the confidential information with a key to create encrypted confidential information;

(c) means for storing the encrypted confidential information;

(d) means for transmitting the key to the client computer;

(e) means for deleting, by the server computer, the key from memory of the server computer;

(f) means for receiving the key associated with the encrypted confidential information from the client during a second communication session; and

(g) means for using the key to decrypt the encrypted confidential information.